Global Information Assurance Certification Paper

SANS GIAC GCFW Practical Assignment (version 4.1)

http://www.giac.org/

By Michael White
Submitted on 2/10/05

Table of Contents

Abstract

This document has three assignments. The first discusses the future state of event collection and correlation. In the second, it talks about the security architecture of a fictional company. It goes into some detail on the various components used to protect it from outside interference. The third and last assignment looks into the specific detail of the firewall and filtering router policies that would be used to protect this fictional company. This fictional company is called GIAC Enterprises and it sells fortune cookie sayings to one and all.

Assignment 1 – Future state of security technology

Event collection and correlation across the enterprise

Abstract: This assignment will examine event collection and correlation in an enterprise paying particular attention to the difficulty involved in doing meaningful analysis of a high volume of events (thousands per minute). A definition of event collection and correlation will be followed by why this subject is important, and then the impact of event collection and correlation on the industry as a whole, and on the individual system administrators will be discussed.

What is an event?

An event is a recorded incident. For example, when a password is changed on a Windows system there will be events recorded with the ID of 627 (password change attempted) and 628[1] (password change successful). An event is a discrete record of some action or activity. A vast amount of information can be produced as events if auditing is not enabled carefully. For example it is possible for auditing to be configured to produce events every time any user opens any file. This can produce so many events that it becomes almost impossible to look at them all. This can be a problem since it is possible to have hidden in all of those events the evidence of a breech of a protected network.

In a corporate environment all of the workstations (Windows and Linux), servers (Windows and Linux), routers, switches, firewalls, and other devices can produce events. Generally speaking all devices produce and store events locally. Therefore, 50 servers will result in at least 50 places to look for events.

What is collection and correlation?

[1] Some of the information on event ID's came from Windows 2000 Auditing and Intrusion Detection, by Microsoft TechNet.

As mentioned above each device in a network can generate events. To make it easier to look at the events they may be collected in one place. In the UNIX / Linux world this can be easily done using something called syslog. However, in Windows there is no tool that can easily do this. Event collection gathers all of the events from the corporation's devices into one place. This also allows correlation, which means that all locked accounts can be reviewed at one time regardless of which server or device the information originated. Often, when information is viewed centrally, it takes on a different importance than when viewed separately. For example, in the Windows world in a collected and correlated database of events, if in the middle of the night a number of 529 events are followed by a 528 event, this may mean that someone was successful at a password attack. This conclusion is valid because 529 means unsuccessful and 528 means a successful authentication. Another example meriting concern and investigation would be if there was an interactive console logon (event ID 540, login type 2) at an odd time on a particularly important server. If it occurred in the middle of the night by a user ID normally used during the day, a crisis may be the logical conclusion. However, if the logs weren't being watched, how would you know?

Why is it important?

It is a dangerous assumption that a system is secure and will not have any security issues. If log files are not being monitored, a security problem will not be identifiable. In addition, log files also point to hardware errors or even service quality issues. However, the problems may not come to light until someone notices that the web server 'looks' different or the admin account is no longer operable. IBM and HP have predictive failure warranties on a variety of hardware. This means you can receive a warranty replacement hard drive or processor, before the one installed in your server dies. The event that says the hard drive is going to die in the future is worth knowing about isn't it?

With deliberate review of the log files, a security breach will be identified closer to the time it occurs. By detecting that a user logged on at an odd time, or that there are a large number of disabled accounts overnight, or that a web server has SYSTEM accessing cmd.exe[2], a potential security issue may be recognized and confirmed. If you don't know what is happening, then you have no chance at all.

It is very difficult to look at each device and its log files to find issues. Some machines, such as Windows server can have normally between 3 and 5 event logs to view and sometimes more. Linux servers generally log to a variety of files locally. Event collection software will roll up all events to one place, easing the detection of potential security breaches.

Typically a successful breach of a perimeter security is preceded by reconnaissance work. The attacker can use tools like Nmap and firewalker to

[2] This suggestion came from How to detect hackers on your web server, by GFI Software on page 5.

build up a picture of the defenses. If all logs are being carefully monitored, a pattern may become apparent in time to block the breach. But if logs are overlooked, nothing will be noticed. In addition, since the all important perimeter defense logs are not being watched, it is likely the logs on the internal servers are also not reviewed. It can be argued that an IDS like Snort (http://www.snort.org) will pick up the traffic that would indicate an attacker is investigating. However, sometimes an IDS is monitored by only one person. If that IDS passed certain alerts up to the event collection point, there may be a number of other people that could respond in a crisis.

If a centralized event collection point exists, and the perimeter security devices roll their events up to it, there is a much better chance that in a crisis there will be someone available, since all of the systems report to the same console. There can be centralized reporting or notification as well.
In an article written by Ka0ticSH[3], he presents a serious approach to detecting a firewall and its configuration, followed by mapping a network out behind the firewall. It is clear and easy to read. It details how to detect the type and configuration of a firewall and then explore behind it. This very powerful knowledge can be used by any computer savvy user. A well thought out and carefully implemented and managed perimeter can minimize the danger from this kind of approach. However, it will be harder to detect and deal with security issues without centralized monitoring.

In case a host is taken over and the logs are removed or modified, an event log in a central location is quite handy. This can be useful for the investigation after the crime is discovered. Sometimes, without centralized event monitoring and correlation it will not be known that a host has been 'lost'.

Why don't more companies do it?

Not everyone has a reason. Often I hear excuses that it is hard or time consuming, or that each server or device must be visited to view the logs. Another excuse is that it is expensive to purchase a tool to make it easier. Another possible excuse is that everything is working and they will worry about it later, at the next budget year.

Another reason is that they are subconsciously afraid. Of what? Take for example: a very small test network with 3 Windows and 3 Linux workstations generates four events that each has a count of 1100 occurrences. Plus there are thousands more events, each with a count of 1 occurrence or more, sometimes with a lot more occurrences. All of this was captured in a two day period. Event collection means to bring all of the events together. But sometimes that is frightening due to the huge number of events that now have to be evaluated. Most of it is chaff, but all of it needs to be examined. Some people will avoid doing event collection and correlation simply due to the fact

[3] Ka0ticSH (asm.coder@verizon.net), "Diggin em Walls – Detection of Firewalls, and Probing networks behind firewalls".

they are concerned about all of the work it can generate.

Another reason that people are not doing more event collection and correlation is they are concerned about the necessary skills. It requires a lot of skill to read the event logs and turn raw data into information. There are tools that will help collect all of the events, and allow one to look at it in different ways, but it still takes skill to take that organized data and turn it into actionable information.

TNT Software ELM Log Manager 3.1 can help

This software has the ability to make the collection of the events on Windows / Linux / UNIX much easier. The events can all be collected in an Access / SQL / Oracle database and then viewed by a number of users through the use of a console application. This MMC based application enables the use of a variety of views and filters to help make the task of correlation easier.

On the http://www.tntsoftware.com web site there is a planning guide (see Appendix for complete URL) that discusses how many events the ELM can handle. While the technical details have not been confirmed it is still a useful guide. On a Pentium II 400 MHz / 256 MB server using SQL Server 2000 locally installed, it could handle up to 40 events per second. This performance was achieved without taxing the processor more than an average of 15% (peak of 18%). This turns out to be 2400 events per minute[4], concluding that ELM can handle significant volume of events.

A simple example of how TLM can help is that a filter can be created that will display only Windows events that have an ID of 529, 531, 539, 532, and 535. These ID's cover invalid user name or password (529), disabled account (531), locked account (539), account expired (532), and password expired (535).

A personal view may be created that only displays events that fit the filter already created above. This view is dynamic. Only the events that fit those simple parameters (failed logins) will be seen. With Windows machines being able to report events in real – time the view may be looked at in real – time to determine which machines were reporting those events. A notification rule could also be easily created, so if one of those events were reported in the view an administrator could be alerted with a page or email. The alert may even result in a response before the person leaves the remote machine! This is useful to security people as well as a help desk.

Another example is to catch people trying to legally access the console of a Linux server. They are not crackers, or hackers, but rather administrators that need to be educated or corrected about something. When they SSH into the console of the Linux machine a syslog event is generated and passed to the ELM server. It is reported in ELM as event 38. A filter for this event and this

[4] This research was done by TNT Software, and published in TNT Software ELM Log Manager Planning Guide on page 9.

server may be easily created. In my testing, it only took 2 or 3 seconds for the syslog on my VMware ESX server (http://www.vmware.com) to generate the event and have it reported to my ELM console. One could also watch for event 86 one second or so before the event 38. It will be an sshd message about accepting the password. But it will also have the IP address for the user. A notification rule can also be built for it so one is paged when it occurs. While there may be other tools that can do this, by using this method there will be records where all of the other records are kept.

With a tool like ELM one console can capture the events from the logs of all perimeter security devices such as firewalls, IDS machines, and edge routers. It will have a significant impact on the security posture as it will allow easy and simplified access to logs that are traditionally not monitored close enough. And sometimes when they are monitored, they are checked one at a time. It will allow system administrators to be more proactive, and when necessary to react much faster.

Tools are not enough

There have been tools available for many years. Tools have been available even longer in the UNIX world. But still they have not been used widely. So it is very clear that tools are not enough. Although newer tools with easy GUI and powerful features can make things much easier, it will still take management and system administrator buy-in to make everything come together.

What is the future?

We know that if we watch our event logs we can find out things like who is trying to break our security, and perhaps even that it has already happened. Even things like a hard drive that is going to die in the future or things like operating system health can be monitored by watching event logs. It is a however, a hard job to wade through all of the data and turn it into information. The tool discussed above can help. But what is really going to make the big difference? Management support is important but will it really make this important task easier and thus have it happen in more companies? Some other changes that would help this are included in the list below.

- More standardization of event descriptions and codes. Windows and Linux for example.
- More available information on events. Microsoft has started this where some events have a URL in them for more information. This could be improved significantly by every event having this URL, and each one having more information available.
- Tools that have more help embedded in them. While tools make working with the data easier, it would be better if they went further. For example, if the tools could connect together events, not only across machines but also operating systems, it would allow system administrators to see more quickly connections that could be ominous. ELM comes with a built-in

KB that is empty. While it is very useful as it is easy to add information to it, and tie it to specific events, it could be enhanced by the addition of information in it.

- There appears to be a potential trend that system administrator skills are improving slowly over time. If this could increase substantially, especially in the areas of security and understanding events, this would make a big change in this area. It would help system administrators convince management of the importance of what they need to do. It would also help get additional budget dollars to assist in purchasing training and tools. A significant result would be system administrators who have more work done in less time, which could help morale, since they are creating a more secure environment. We all know that more secure environments work better!

It is quite exciting to think about how these tools and improvements, together with management support could possibly increase the number of organizations that practice event collection and correlation. If this were to happen a likely direct result of it would be potentially more secure organizations. This would hopefully result, because as a system administrator becomes more aware of what is happening they would fix things more often, since they know about them, and less security breaches would occur. Another potential benefit is that as system administrators know more generally, and learn more about their organization, it is possible that they would understand even better the importance of patching and minimum security baselines, and this would make more secure computers and networks. An end result of these changes would be healthier and more secure corporate networks which could result in a healthier and more secure Internet, as well as generally healthier corporate networks.

These changes and improvements would also improve system administrator morale since they will be able to more easily be aware of the condition of their network and in fact become more proactive. Better morale is often something that helps improve productivity.

Summary

I have discussed the feasibility of high volume event collection and correlation and how it can help companies be more secure and proactive. I conclude that high volume event collection and correlation is not only possible, but that there are tools that can assist in the collection of the huge amount of event data and turn it into useful information. I have also concluded that tools alone will not help. We need management support, as well as system administrator support. Improved tools and management support would make significant improvements in the overall industry wide acceptance of doing this important activity. I also believe that the health of our Internet and corporate networks could be improved by this important task.

Assignment 2 – GIAC Enterprises Security Architecture

Abstract: This assignment will define the security architecture that GIAC will use to not only secure itself but to support the growth of the company as it increases its business on the internet. It will cover a philosophy that IT staff will always be aware of, as well as the individual components and the relationships between the components. Staffing responsibilities will also be covered as well as training.

What is GIAC Enterprises?

This is a small business that markets fortune cookie sayings to customers all over the world. Most of the fifty employees work at the head office, but there are four regional satellite offices. These very small offices are used by sales people to generate business. All of the sales are handled via the Internet. This is true whether remote sales people make the sale, or it happens via the web presence.

IT Security Philosophy

The following is a very important theme that all IT people will understand and work within.

"The company makes its money electronically. For this to happen there are many systems that must work together securely. IT security is what will allow that to happen safely. All of our work must be done while thinking of simplicity, defense in depth, and that the business must go on. We must err on the side of security, but always remember that our business must work for all of us to succeed."

Defense in depth is part of the security thinking. There are a multiple of layers in a variety of areas. Security is built in everywhere. For example, GIAC has chosen not to use Microsoft Exchange. This was not only a security decision of course, but IT Security was part of it. GIAC uses IBM Lotus Domino as a result of a detailed evaluation that was partially made up of security research.

While perimeter security is important, so is security throughout the enterprise. For example anti – virus on all machines, or not putting up network diagrams where anyone can see them. Another example uses Microsoft's Active Directory (AD) to enable and manage the Windows firewall on PC's and servers.

In addition, once per month there is a lunchtime seminar (GIAC supplies pizza & pop), and several times per year there are security related presentations. The next one is "Why NOT to use passwords but passphrases instead". The following one is "How to be CyberSafe at home". These seminars have

handouts and specific suggestions.

IT Strategy

The IT Strategy impacts much of what is discussed in this document. It is what gives direction where there isn't necessarily any.

Passwords

GIAC teaches users not to use passwords but instead use passphrases. There are password complexity parameters in use for all systems. Normal users have their passphrases changed every 75 days. While this is not ideal, it was what was negotiated with management. It allowed 15 character passphrases. All users have been taught to work with this effectively. Through the use of passphrases it makes the change cycle (75 days) much more palatable. Users with system administrator type access have a monthly change cycle.

Anti – Virus

Every computer must have anti – virus (AV) installed, properly configured, and locked down. This includes laptops, servers, file / print servers, groupware servers, and SQL servers. There must be daily updates (when it is available), as well as centralized reporting of virus strikes. Only the lead IT security administrator will be able to disable AV software and it will have to be documented each time. Groupware servers will need to have OS level of AV and AV within the Groupware environment. All HTTP streams into the company must be checked with AV software. Symantec Antivirus (SAV) 9.02 is in use on servers and workstations. YYCIT1 is the server that hosts SAV and its management console. Symantec Message Security for Domino (SMS) v4.1 is in use on the groupware server. There is also AV installed and running on the Symantec firewall (YYCFW1) that is used to check HTTP, SMTP and FTP traffic into the company.

Active Directory

All users and computers are part of a Windows 2003 domain. With workstations running XP SP2 and servers running Windows 2003, active directory is heavily used. Each server and workstation has the Windows firewall running and configured to only allow the traffic that is expected for that workstation.

Work Journal

Each of the important security elements have an assigned work journal that must be used to record changes. These journals will be considered security assets and protected as such. They will be useful for change tracking and problem determination. The devices that will have a work journal assigned are: YYCRT1, YYCFW1, YYCIT3, YYCIT4, and YYCIT1.

This journal will track things like patches / hot fixes applied, configuration changes, significant incidents, and the date / time and author of the change. They will be kept out of sight during work hours and under lock outside of work hours.

Roles that interact with the Security Architecture

There are number of roles that interact with the GIAC security architecture. To maintain and improve the systems, these roles must be fully understood. Anyone or anything that doesn't fit into one of these roles is not allowed into the systems.

IT Security Staff

In the very small IT department at GIAC there is one dedicated IT Security person. At time of hire he was a Windows 2000 MCSE with experience in Windows and Linux. He was also a SANS graduate in GSEC. His future growth path includes additional certification with SANS (GCFW – URL in Appendix) and Symantec (very long URL in Appendix).

The job includes dealing with the obvious such as the firewall and SNORT IDS equipment but also helping to make sure that the minimum security baseline (MSB) was appropriate for the workstations and servers, both from function and security viewpoints. The YYCIT1 server was dedicated to security, and he was responsible for using the ELM (http://www.tntsoftware.com) event collection and correlation tool that was installed on it to monitor the logs and events on the security equipment as well as the internal servers and workstation. This tool was used by the other IT staff as well for non – security specific tasks. The SNORT install at GIAC is still very new to the security staffer. It is a work in progress but it is improving fast.

The IT Security person is also responsible for using Retina[5] and Nmap[6] on a regular basis (monthly) to make sure nothing is missed. The Retina vulnerability scanner is easy to use and will produce reports that will be kept and used for comparison purposes. This tool is used when MSB's are created to make sure that they are well defined.

Customers

These are the people and organizations that purchase bulk orders of fortunes from GIAC. All of their business originally started either from phone or email. Once a relationship was established (including a credit check) they were provided with an account and password that would be used to authenticate over the Internet (account was emailed, and password was provided by courier). They were also provided a SSL client certificate that they would have to import into their browser once and it would be part of the authentication process. The

[5] Retina is a network vulnerability scanner from eEye Digital Security – www.eeye.com.
[6] Nmap is a network security scanner from Fyodor at www.insecure.org.

first time they authenticated they were forced to change their password – and it had to match the same complexity requirements of the internal users. Note: the client certificate is created and managed through the PKI installed as part of the Lotus Domino environment on YYCDOM1.

They will connect to GIAC through HTTPS but will only be able to do that from a browser that has the client certificate installed in it. The SSL will be used for encryption, and the certificate / account / password will be used for authentication. They will connect to a Domino server in the Service network running HTTP. It will host a Domino database that will communicate as required to the Domino server on the internal LAN.

Source	Destination	Port(s) Protocol	Description
Customers	Web server	443/TCP (HTTPS)	Customer access to web server to view catalog, place orders, view order status, etc.
Customers	Mail server	25/TCP (SMTP)	SMTP mail access.

Suppliers

Suppliers are the companies that supply GIAC with fortune cookie sayings. All of their business originally started either from phone or email. Once a relationship was established (including a credit check) they were provided with an account and password that would be used to authenticate over the Internet (account was emailed, and password was provided by courier). They were also provided a SSL client certificate that they would have to import into their browser once and it would be part of the authentication process. The first time they authenticated they were forced to change their password – and it had to match the same complexity requirements of the internal users.

They will connect to GIAC through HTTPS but will only be able to do that from a browser that has the client certificate installed in it. The SSL will be used for encryption, and the certificate / account / password will be used for authentication. They will connect to a Domino server in the Service network running an HTTP task. It will host a Domino database that will communicate as required to the Domino server on the internal LAN.

Source	Destination	Port(s) Protocol	Description
Suppliers	Web server	443/TCP (HTTPS)	Supplier access to web server to view order information.
Suppliers	Mail server	25/TCP (SMTP)	Mail access.

Partners

The organizations that translate and resell GIAC fortune cookie sayings are called partners. All of their business originally started either from phone or email. Once a relationship was established (including a credit check) they were provided with an account and password that would be used to authenticate over the Internet (account was emailed, and password was provided by courier). They were also provided a SSL client certificate that they would have to import into their browser once and it would be part of the authentication process. The first time they authenticated they were forced to change their password – and it had to match the same complexity requirements of the internal users.

They will connect to GIAC through HTTPS but will only be able to do that from a browser that has the client certificate installed in it. The SSL will be used for encryption, and the certificate / account / password will be used for authentication. They will connect to a Domino server in the Service network running HTTP an HTTP task. It will host a Domino database that will communicate as required to the Domino server on the internal LAN.

Source	Destination	Port(s) Protocol	Description
Partner	Web server	443/TCP (HTTPS)	Partner access to web server to view catalog, place orders, etc.
Partner	Mail server	25/TCP (SMTP)	Mail access.

GIAC Enterprises remote users

There are a number of outbound sales people that are based outside of the corporate headquarters. They each have a laptop that has a VPN client that connects them to the LAN in the main office. They mostly work with the Groupware server – YYCDOM1. The traffic with the groupware server could be encrypted, but since it will be encrypted over the VPN it will not be encrypted by Domino as well. The Notes client on their laptop has all of the company databases encrypted with medium grade encryption. There is additional field level encryption in applications where appropriate. While these laptops are outside of the office, they are still partially managed. They are not subject to the same limitations that the internal workstations are, such as the Windows firewall – since they have a personal firewall in use. However they have Symantec AntiVirus installed and are managed the same as the internal users. In addition, the Symantec Client Firewall (SCF) is also installed. Both it and SAV are managed by the console on YYCIT1.

Source	Destination	Port(s) Protocol	Description
Remote Users (Sales)	LAN Resources	50/IP (ESP) , 51/IP (AH)	VPN access

Remote Users (Sales)	LAN Resources	500/UDP (IKE)	IKE permits key negotiation for VPN setup.
Remote Users	LAN Resources	139/TCP, 137/UDP, 138/UDP, 445/TCP	File and print server services, Windows networking.
Remote Users	Domino server	1352/TCP (Lotus Notes)	Mail and groupware access
Remote Users	Various – local subnet only.	53/UDP, 53/TCP (DNS)	Name resolution

GIAC Enterprises internal users

The internal users interact with the corporate systems mostly through Lotus Notes and Domino. The order taking system is a Domino database that is hosted internally. Where it is necessary due to relational data requirements, the SQL server is configured to allow the Domino server to communicate with it.

The internal users will be able to browse the Internet (HTTP / HTPS). They will not be able to access restricted sites or subjects. This will be managed by content filtering technology on YYCFW1.

Source	Destination	Port(s) Protocol	Description
Internal Users	Various – local subnet only.	139/TCP, 137/UDP, 138/UDP, 445/TCP	File and print server services, Windows networking.
Internal Users	Internal web server	80/TCP (HTTP)	Intranet web server.
Internal Users	Domino server	1352/TCP (Lotus Notes)	Mail and groupware access
Internal users	Various – local subnet only.	53/UDP, 53/TCP (DNS)	Name resolution
Internal users	Various external web sites	80/TCP (HTTP), 443/TCP (HTTPS)	General web browsing.

Note: Most of this access is managed in AD using the Windows Firewall.

The General Public

Users on the Internet can connect to GIAC web server (HTTP / 80) to see some corporate public relations type data. It includes where they can buy fortune cookies that have GIAC sayings in them as well as some sample sayings.

Source	Destination	Port(s) Protocol	Description

General Public	Web server in service network.	80/TCP (HTTP)	To browse PR data.
General Public	Mail server.	25/TCP (SMTP)	Mail services.

Security Components

IP Scheme

Inside the LAN the following IP scheme is in use.

- 192.168.9.x / 24
- Default gateway is 192.168.9.1
- Routers have 192.168.9.1 - .19
- Servers have 192.168.9.20 - .49
- Printers have 192.168.9.50 - .69
- DHCP for workstations have 192.168.9.70 - .135

The firewall Service Network uses 192.168.10.x /24. The network between the firewall (YYCFW1) and the edge router (YYCRT1) uses 68.10.187.113 - .126 /28. The outside of the router has 68.10.187.97 - .110 /28.

The IP information is available on the network diagram that is available in the Appendix.

Filtering Router – YYCRT1

The router is the last step before information leaving GIAC reaches the Internet. Conversely it is the first step for information leaving the Internet bound for GIAC. The philosophy for this router is for it to be an absolute filter on the traffic. Anything that can always be blocked without exception will be blocked by this device. This is a Cisco router model 1721 with IOS version 12.2. This router will be used to do packet filtering. It will be useful for things such as ingress and egress filtering to help block traffic from networks that never should have entered the network, for example, private IP addresses and loopback addresses[7]. Since it is on the edge of GIAC, it will block traffic before it even gets to the firewall, so that the firewall can deal with the more appropriate traffic that for example requires stateful inspection or application proxy. This product can be said to have a lot of weakness, since it is not stateful, nor can it inspect packets, but these are also its strength. It may not do as much, but it does it fast.

This router was chosen after research on the Cisco web site. It would work well for the current DSL connection, but could be upgraded in the future to additional capabilities.

This router will only be accessible via SSH from inside the company (on specific IT Security admin workstation(s)), or via serial cable if necessary.

[7] As discussed in Help Defeat Denial of Service Attacks: Step-by-Step, by the SANS Institute.

For the writing of this document a real router was not available for testing. If one was, the National Security Agency Cisco Security Recommendation Guide would have been used to help secure the router. In addition, the Router Audit Tool from the CIS would have been used to test the policy. The URL's for these tools are in the Appendix.

Firewall – YYCFW1

This is a Symantec Security Appliance, model SGS 5420 version 2.01 (see the Appendix for a URL). This firewall is used to perform a variety of tasks. Aside from the firewall function, it also does Antivirus (AV) for HTTP, FTP, and SMTP traffic. It also does Intrusion Detection (IDS) (which includes protocol anomaly, signature and traffic anomaly detection) and Intrusion Prevention (IPS) (which includes gating and blacklisting). The firewall is a full inspection firewall that inspects packets at the IP layer, circuit layer, and application layer and provides deep packet inspection and enforces RFC compliance[8]. YYCFW1 will inspect all traffic that is passed to it. It will block all traffic that is not explicitly allowed. In addition, any traffic that should be blocked for other reasons, such as virus infected email, file attachments, or HTTP traffic; while the traffic may be legal it will still be blocked. The weakness of this type of application proxy firewall is often performance. This will be offset somewhat by having the filtering router block a lot of traffic. In addition it will only stop HTTP attacks that it recognizes. If HTTP traffic is legal, but devious in nature, and not recognized by the firewall, it will pass through. However by having all of the workstations and servers installed to a secure standard (MSB), it will help mitigate the possible damage. In addition, another layer of protection is provided by AV on all workstations and servers.

This firewall has the ability to perform 'split – DNS' services. This means the internal DNS information will not make it out to the public. The outside DNS is limited to zone transfer with the externally hosted (http://www.easydns.com) DNS backup. The firewall will limit zone transfers from happening except with the externally hosted DNS at EasyDNS. In addition, this firewall has an application proxy for SMTP (and HTTP) which also allows for virus and content filtering. Both of these functions will be used.

The firewall provides NTP time services to the LAN, and it talks to a variety of time servers to make sure the time is consistent and accurate. The clock for all of the workstations / servers is provided by their domain controller (YYCIT2) and it gets its time from the firewall. The Linux server gets its time from the firewall.

This firewall product was chosen due to previous experience with Symantec and Axent. It integrates with management products that integrate with the desktop, server and groupware AV, as well as third party products. The decision to go with Symantec was made before the firewall choice was made. It was very attractive that this one device was an appliance and that it could do more than

[8] This description is from the Symantec Security Appliance comparison chart, by Symantec.

just firewall functions. While this can sometimes be a negative feature, it was concluded that since the additional functions were core Symantec capabilities, it would work well together. To mitigate any possible issues in this area, all of the servers and workstations have AV installed and Windows firewall running. In addition there is aggressive patch management and AV in the groupware.

VPN

The VPN is used to provide the remote sales force with access to the internal LAN. They will work with YYCDOM1 mostly which hosts all of the databases that they require access to, as well as email and related applications. The Symantec Enterprise Client VPN v8.0 is used on the remote machines. The firewall that is hosting the VPN can handle 90 Mbps of 3DES encrypted traffic (with 95 Mbps of full inspection). With the VPN providing secure LAN access to the remote users, it will allow AD to control a variety of features on their workstation, such as Automatic Updates and the Symantec console to control the SAV / SCF clients installed on their laptops.

Network based IDS

This is installed on YYCIT4 which is a Red Hat Linux (v9) server. It has been installed very carefully so that it only has what is required. It was installed with a purchased copy of Red Hat, and the Red Hat Network is used to keep it patched regularly. In addition, Retina was used to help make sure it had no vulnerabilities that were unexpected or avoidable. Its syslog is pointing at YYCIT1. While the onsite staff is using this project to explore IDS and Linux, they have had some experience previously. They used the Bastille project script (http://www.bastille-linux.org/) to secure the box. Currently, this PC has the SNORT sensor and server installed on it. SNORT was installed using the guidelines in the book Intrusion Detection with Snort by Jack Koziol.

This machine is used to provide information on attacks that make it through the firewall. In addition, if there is a virus breakout within the company and for some reason SAV is not able to tell where it is coming from (using its Threat Tracer feature), then SNORT hopefully will. From the position where it is attached to the LAN, it will not be able to monitor between the filtering router and the firewall. If there was a sensor outside the firewall it would generate a great deal more activity and the skill set of the operators may (would) not have been ready for it. It was partially a cost decision to go with SNORT, however even a small amount of research shows that SNORT has a good reputation – not for install or administration, but for functionality. It was decided this was a low cost way to start looking at IDS and Linux technology. If it works well, and the IT Security staff is happy with it, there will likely be additional sensors added. Probably one in the Service network, and one plugged into a mirrored (switched port analyzer port) port on the switch the servers are plugged into. This is easy to predict due to the cost of implementing these changes.

IT Security Server – YYCIT1

This server hosts the Windows console for SNORT. It also hosts the ELM application that is the event collection and correlation software. It is the central repository for all Windows and Linux events and logs. In addition it receives SNMP alerts from the firewall (YYCFW1) and edge router (YYCRT1). It also hosts the Symantec AV console which holds the centralized reporting and configuration management for the AV / personal firewall clients. The Microsoft product Software Update Services (SUS) is also installed on this server.

Patch Management

At GIAC Enterprises patch management is seen as an integral part of IT security. While the IT Security staff member may not do the work of patching, he is responsible for it being done. To make it as easy as possible, the company is using Microsoft's SUS on workstations with automatic install. While this may seem risky, it has been working very well. Approval for the patch is centralized at the SUS console so patches are not in theory approved until they have been tested. This is also in use on the servers; however, it is not automatically installed. The approved patches are downloaded so that it is ready to go. Then at the next login when there is an outage window, the patch is installed and restarted if necessary.

On the Linux server (YYCIT4) the Red Hat network is used to keep patches current.

The email / groupware environment has its own tools to keep clients current, and the two servers are not hard to manually update, so they all are kept within 30 – 45 days of the current release, although in the case of Fix Packs they are upgraded sooner.

The Windows server in the service network is very locked down. It has the Windows firewall installed and configured. However any critical Microsoft or IBM / Lotus patches are downloaded to CD and installed on that machine at the earliest possibility.

Future Improvements

Some of the things that could be looked at in the future that may improve security or administration, or perhaps only save money are outlined below. They are only ideas that may be worthy of consideration – although some of them are very good ideas that will likely be installed in the short term.

No more VPN

One of the things to look at in the future is the removal of VPN's. This could be safely done by having the Sales force connect to the Domino server in the service network. It could pass their connection through to the Domino server in the LAN. This would potentially slightly simplify things. It would save money as well, since VPN capabilities in the firewall would not have to be licensed or

supported. Removal of VPN's is not likely as it would remove the ability to manage the personal firewall and antivirus clients on the remote user's laptop as well as remove the possibility of using the VPN for other tasks.

More VPN

It may be a good idea to have some IT staff with the ability to work at home on the corporate LAN. This could help improve response time in a crisis as well as help morale. It would also help the IT staff keep its skill sharp with the VPN usage so that they could support their users better. After the new domain controller, this is likely the next most important improvement.

Add second firewall

There may be a case to improving security if there were two firewalls in use at GIAC. This would mean having an inner and outer firewall with the service network on the inside.

Additional controls for VPN users

The Symantec VPN may allow for checks to be done on the clients before they are connected to the corporate LAN. This should be explored to see what / if it offers anything. It may be a way to block remote users from connecting if there are missing patches.

Additional ISP

A future project is to look at implementing something like a Radware (http://www.radware.com) box to allow the use of two ISP's connected to the corporate network, but yet be simple to manage and provide failover outgoing and incoming.

Additional Domain Controller

This is likely one of the first next projects. There should always be at least 2 domain controllers, but it was not possible initially. The additional controller would host DNS as well as a backup DHCP scope.

Assignment 3 – Router and Firewall Polices

As two of the key components in the perimeter defense of GIAC Enterprises the router (YYCRT1) and firewall (YYCFW1) configuration is very important. Below is the configuration of both. This configuration was not tested on the actual devices since neither was available. As was mentioned previously, if the real router was available, the Router Audit tool (RAT) from http://www.cisecurity.org would have been used to test this configuration.

YYCRT1 Configuration

Below is the configuration of the GIAC filtering router YYCRT1. It is a Cisco 1721. In this configuration the firewall (YYCFW1) will be allowed to manage ICMP traffic using its PING proxy. This will allow the support staff to easily turn on or turn off PING support as required.

YYCRT1

```
Interface Ethernet 0
        ip address 68.10.187.97 255.255.255.240
        ip access-group 101 in

Interface Ethernet 1
        ip address 68.10.187.113 255.255.255.240
        ip access-group 102 in

service password-encryption
hostname yyctr1
no ip redirects
no ip directed-broadcast
no ip unreachables
no ip proxy-arp
no cdp enable
no cdp run
no ip finger
no ip http server
no ip route-cache
no ip mroute-cache
no ip source-route
no ip mask-reply
ip tcp synwait-time 10
scheduler interval 500
service password-encryption
no service udp-small-servers
no service tcp-small-servers
no ip bootp server
logging trap warnings
logging 68.10.187.114
ip audit notify log
ip audit po max-events 100
ip cef
aaa new-model
aaa authentication login default local
aaa authentication enable default enable
aaa session-id common
enable secret 5 $1$VZAc$KDeobDIp6EqETuYWmM8AA1
```

```
ip ssh time-out 60
ip ssh authentication-retries 2
ip domain-name giac.com
no ip identd
clock timezone MST7DST -7
ntp server 136.159.2.2
ntp server 128.100.103.252
ntp server 132.246.168.148

access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 224.0.0.0 31.255.255.255 any log
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip 0.255.255.255 0.0.0..0 any log
access-list 101 deny ip 255.255.255.255 0.0.0.0.0 any log
access-list 101 deny ip any host 68.10.187.97 log
access-list 101 deny ip any host 68.10.187.113 log
access-list 101 deny tcp any any range 135 139
access-list 101 deny udp any any range 135 139
access-list 101 deny tcp any any eq 445
access-list 101 deny tcp any any range 6000 6255 log
access-list 101 deny udp any any eq 69 log
access-list 101 deny udp any any eq 514 log
access-list 101 deny udp any any range 161 162 log
access-list 101 deny icmp any any host-redirect echo
access-list 101 permit tcp any any
access-list 101 permit udp any any
access-list 101 permit ip any any


access-list 102 deny tcp any any range 135 139
access-list 102 deny udp any any range 135 139
access-list 102 deny tcp any any eq 445
access-list 102 deny tcp any any range 6000 6255 log
access-list 102 deny udp any any eq 69 log
access-list 102 deny udp any any eq 514 log
access-list 102 deny udp any any range 161 162 log
access-list 102 deny icmp any any echo-reply unreachable
access-list 102 permit tcp 68.10.187.114 0.0.0.15  any
access-list 102 permit udp 68.10.187.114 0.0.0.15 any
access-list 102 permit icmp 68.10.187.114 0.0.0.15  any
access-list 102 permit ip 68.10.187.114 0.0.0.15 any
access-list 102 deny any log-input
```

YYCFW1 Configuration

Below is the configuration of the GIAC firewall YYCFW1. It is a Symantec 5420 appliance. The firewall rule base is not order dependent but rather best fit[9].

Everything in this firewall is blocked by default. In fact, there is no routing of TCP/IP at any layer except for the application layer by the firewall. This means if there is no rule, there is no traffic passing.

In the chart below an **Inspect type** of Full means Application Data Scanning, which allows the firewall to pass traffic to anti – virus scanning or content filtering as appropriate as well as passing through an application proxy. When the traffic is not passing through an application proxy it is labeled as stateful. All traffic is logged. While HTTP traffic is being checked for virus infected traffic, it is also being checked for known attack signatures and if found then blocked.

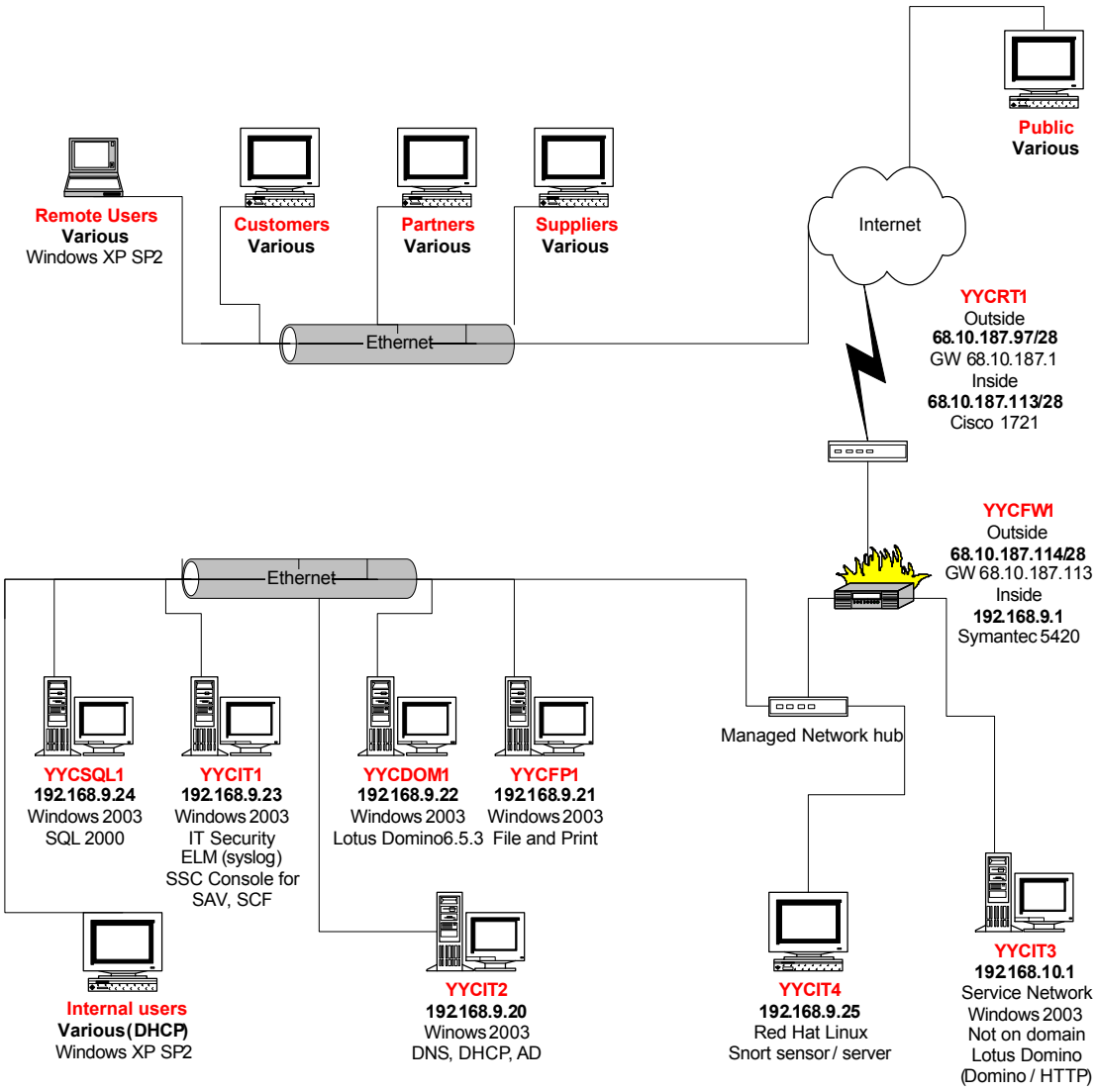
Number	Source	Destination	Protocol	Inspect type	Action	Comments
1	InsideAdmin Workstations	YYCFW1	HTTPS	Full	Allow	Firewall management
2	YYCFW1	EasyDNS	DNS	Full	Allow	Zone Transfer with DNS backup – www.easydns.com
3	YYCFW1	Outside	DNS	Full	Allow	DNS lookups.
4	Outside	YYCDOM1	SMTP	Full	Allow	The firewall scans traffic for malware and illegal traffic. Only accepts mail for GIAC.com. No source routes are accepted and mail only accepted from known domains. Also known relay servers database sbl-xbl.spamhaus.org is checked.
5	Outside	YYCIT3	HTTP	Full	Allow	Public web site in service network.

[9] See the Additional Information section of the Appendix for a very long URL to learn more about rule processing in Symantec firewall products.

6	Outside	YYCIT3	HTTPS	Full	Allow	Partners, customers, supplier access. Private part of public web server. Requires HTTPS, certificate, and account / password for access.
7.	Outside	Inside	ICMP	Full	Block	Ping not allowed in.
8	Inside	Outside	ICMP	Full	Allow	Ping is allowed to travel out.
9	Inside	YYCIT3	3389/TCP	Stateful	Allow	RDP to service network server.
10	YYCIT3	YYCDOM1	1352/TCP	Stateful	Allow	Access to main domino apps for order management.
11	YYCIT2	YYCFW1	DNS	Full	Allow	DNS lookups.
12	InsideAdmin Workstation s	YYCRT1	SSH	Stateful	Allow	SSH access to edge router.
13	Outside	YYCFW1	500/UDP, 50/IP, 51/IP	Stateful	Allow	VPN for sales staff.
14	YYCRT1	YYCFW1	514/UDP	Stateful	Allow	Redirected to YYCIT1 – syslog server.
15	YYCFW1	YYCIT1	514/UDP	Stateful	Allow	YYCIT1 is syslog server.

Appendix

GIAC Network Diagram



References

The following materials were consulted during the preparation of this document.

- TNT Software, ELM Log Manager 3.1 Planning Guide - https://www.tntsoftware.com/Products/ELM/Download.aspx?file=ELMPlanningGuide.pdf, 1/25/05

- The SANS Institute, Help Defeat Denial of Service Attacks: Step-by-Step, - http://www.sans.org/dosstep/index.php

- GFI Security & Messaging Software, How to detect hackers on your web server - http://www.gfi.com/whitepapers/detect-hackers-on-web-server.pdf, 1/23/05

- Microsoft TechNet, Windows 2000 Auditing and Intrusion Detection, 2/10/04 - http://www.microsoft.com/technet/security/guidance/secmod144.mspx, 1/24/05

- Ka0ticSH (asm.coder@verizon.net), "Diggin em Walls – Detection of Firewalls, and Probing networks behind firewalls", New Order – computer security and networking portal, http://neworder.box.sk/newsread_pring.php?newsid=2914

- The SANS Institute "SANS GIAC training". Firewalls, Perimeter Protection & VPNs, Module 2.2 Packet Filters, SANS Press.

- Symantec, "Symantec Security Appliances", http://enterprisesecurity.symantec.com/content/displaypdf.cfm?PDFID=685

- Jack Koziol, Intrusion Detection with Snort, Sams Publishing, 2003

URL's for additional information

These URLS below can be used for follow-up information on various subjects.

- Symantec Certification Services - http://www.symantec.com/education/certification/index.html

- SANS GIAC Information - http://www.giac.org/certifications.php

- Symantec Gateway Security 5400 Series - http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=133

- Rule Processing Information for Symantec 5420 - http://service1.symantec.com/support/ent-gate.nsf/d5cb439a8037087388256d90004bd112/f0979f8de8501b7588256d7b005a2469?OpenDocument&prod=Symantec%20Gateway%20Security&ver=2.0.1%20-%20Model%205400%20Series&src=ent&pcode=sym_gateway_security&dtype=corp&svy=&prev=&miniver=sym_gw_security_201_5400

- National Security Agency Cisco Security Recommendation Guide – http://nsa2.www.conxion.com/cisco

- Router Audit Tool from Center for Internet Security – http://www.cisecurity.org/sub_form.html